



# CVE-2020-10701

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-10701
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-27 19:15:00 UTC
<b>Updated</b>	2022-05-13 20:47:00 UTC
<b>Description</b>	A missing authorization flaw was found in the libvirt API responsible for changing the QEMU agent response timeout. This f

## Risk And Classification

**Problem Types:** CWE-862

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Libvirt	All	All	All	All

## References

Reference	Source
CVE-2020-10701 Libvirt Vulnerability in NetApp Products   NetApp Product Security	CONFIRM <a href="#">s</a>
1819163 – (CVE-2020-10701) CVE-2020-10701 libvirt: guest agent timeout can be set under read-only mode leading to DoS	MISC <a href="#">t</a>
CVE Program record	CVE.ORG <a href="#">v</a>
NVD vulnerability detail	NVD <a href="#">r</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[900190](#) CBL-Mariner Linux Security Update for libvirt 6.1.0

[900919](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (6657-1)

[903260](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (4318)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**